What is claimed:

1   1.   A method for forming a strong password comprising the steps of:

2   obtaining biometric data from a user;

3   generating a one-time password for the user; and

4   combining the biometric data and the one-time password to form the
5   strong password.

1   2.   A method according to claim 1, further comprising the step of
2   encrypting the combined one-time password and biometric data using an encryption
3   key to form the strong password.

1   3.   A method for controlling access to secure data comprising the
2   steps of:

3   receiving a strong password including one-time password and biometric
4   data from a user;

5   separating the one-time password and the biometric data;

6   comparing the one-time password to a calculated one-time password to
7   determine if the one-time password is valid;

8   determining a probability that the biometric data is from the user;

9   encrypting the secure data using an encryption key to obtain encrypted
10 data if the one-time password matches the calculated one-time password and the
11 probability that the biometric data is from the user exceeds a predetermined threshold
12 value;

13   combining the strong password, the encryption key and the encrypted

14   data; and

15   transmitting the combined strong password, encryption key and

16   encrypted data to the user.

1   4.   A method according to claim 3, further including the step of

2   encrypting the combined strong password and encryption key using a further

3   encryption key.

1   5.   A method according to claim 3, wherein the secure data includes

2   items having respectively different security levels, and the step of encrypting the

3   secure data aborts the method if either the one-time password does not match the

4   calculated one-time password or the probability that the biometric data is from the

5   user does not exceed the predetermined threshold value.

1   6.   A system for implementing secure access to a remote computer

2   system comprising:

3   at least one first computer securely coupled to the remote computer

4   system;

5   at least one second computer coupled to said at least one first computer

6   and configured to obtain identifying information from a user;

7   whereby the second computer passes the identifying information to the

8   first computer, the first computer passes the identifying information to the remote

9   computer system and the remote computer system verifies the identifying information.

1   7.   A system according to claim 6, wherein the identifying

2   information is a strong password including a one-time password and biometric

3   information.

1   8.   A system according to claim 7, wherein the identifying
2   information is encrypted with an encryption key.

1   9.   A system according to claim 8, wherein the at least one second
2   computer is securely connected to said at least one first computer by means of a
3   Secure Socket Layer connection.

1   10.   A system according to claim 9, wherein the at least one second
2   computer includes a further Secure Socket Layer connection for receiving the
3   identifying information from the user.

1   11.   A system according to claim 9, wherein the remote computer
2   includes firewall software through which the at least one first computer is coupled to
3   the remote computer.

1   12.   A method of allowing access to secure data on a remote
2   computer, including the steps of:

3   a) receiving a request from a user to access the secure data at a first
4   computer;

5   b) transferring the request to access the secure data from the first
6   computer to a second computer;

7   c) transferring the request to access the secure data from the second
8   computer to the remote computer;

9   d) authorizing access to the secure data at the remote computer;

10   e) transferring the secure data to the second computer; and

11   f) transferring the secure data from the second computer to the user
12   without using the first computer.

1   13.   A method according to claim 12, wherein the request to access

2   the secure data includes a strong password and step e) includes the steps of:

3   encrypting the secure data with an encryption key;

4   combining the encryption key with the strong password;

5   encrypting the combined encryption key and strong password with a

6   further encryption key; and

7   transferring the encrypted combined encryption key and strong password

8   and the encrypted secure data to the second computer.

1   14.   A method according to claim 13 wherein the step of encrypting

2   the data with an encryption key includes encrypting the data with a symmetric

3   encryption key and the step of encrypting the combined encryption key and strong

4   password with a further encryption key includes the step of encrypting the combined

5   encryption key and strong password with an asymmetric encryption key.

1   15.   A method according to claim 14, wherein the strong password

2   includes a one-time password and biometric information and the step d) includes the

3   steps of:

4   separating the one-time password and the biometric information;

5   comparing the one-time password to a calculated one-time password;

6   determining a probability that the biometric information matches an

7   authorized user; and

8   authorizing access to the secure data only if the one time password

9   matches the calculated one-time password and the probability that the biometric

10   information matches an authorized user exceeds a predetermined threshold value.

1 16.   A computer readable carrier including computer program
2 instructions that cause a computer to form a strong password comprising the steps of:

3 obtaining biometric data from a user;

4 generating a one-time password for the user; and

5 combining the biometric data and the one-time password to form the
6 strong password.

1 17.   A computer readable carrier according to claim 16, wherein the
2 computer program instructions further cause the computer to perform the step of
3 encrypting the combined one-time password and biometric data using an encryption
4 key to form the strong password.

1 18.   A computer readable carrier including computer program
2 instructions that cause a computer to implement a method for controlling access to
3 secure data comprising the steps of:

4 receiving a strong password including one-time password and biometric
5 data from a user;

6 separating the one-time password and the biometric data;

7 comparing the one-time password to a calculated one-time password to
8 determine if the one-time password is valid;

9 determining a probability that the biometric data is from the user;

10 encrypting the secure data using an encryption key to obtain encrypted
11 data if the one-time password matches the calculated one-time password and the
12 probability that the biometric data is from the user exceeds a predetermined threshold
13 value;

14   combining the strong password, the encryption key and the encrypted

15   data; and

16   transmitting the combined strong password, encryption key and

17   encrypted data to the user.

1   19.   A computer readable carrier according to claim 18, wherein the

2   computer program instructions further cause the computer to perform the step of

3   encrypting the combined strong password and encryption key using a further

4   encryption key.

1   20.   A computer readable carrier according to claim 19, wherein the

2   secure data includes items having respectively different security levels, and the

3   computer program instructions further cause the computer to perform the step of

4   aborting the method if either the one-time password does not match the calculated

5   one-time password or the probability that the biometric data is from the user does not

6   exceed the predetermined threshold value.